WHAT IS CLAIMED IS:

1. A secure electronic content system, the system comprising:

a controller including an interface component;

a host system coupled to the controller, the host system configured to present content under predetermined conditions, the host system operable with a navigation protocol, the host system further including a system manager operable with:

an associations component configured to be at least partially run by the host system;

a translator configured to provide meanings and generate commands within the host system;

at least a first digital rights management (DRM) component configured to provide encoding and access rules for the content; and

a file system component including a file system application programming interface (API) configured to provide a logical interface between a plurality of components.

2. The system of claim 1 further comprising a medium operable with the host system and the controller, wherein the medium holds the content in files accessible via one or more of the first DRM component, the file system component, and a second DRM component.

3. The system of claim 1 wherein the content is governed by one of the first DRM component in conjunction with a second DRM component, by the first DRM component, and by the second DRM component in conjunction with the file system component.

4. The system of claim 3 wherein the first DRM component governs access to pre-recorded content on a medium via a secure application programming interface (API).

5. The system of claim 3 wherein the second DRM component governs access to pre-recorded content on a medium via a secure application programming interface (API) associated with the first DRM component.

6. The system of claim 1 wherein the host system is operable with a computer system, the host system preventing access to the content by the computer system.

7. The system of claim 2 wherein the medium operable with the host system and the controller is a media disk.

8. The system of claim 1 wherein the host system further includes an engine component, the engine component including predetermined metadata inaccessible outside the engine, the engine configured to provide a security layer of encryption.

9. The system of claim 1 wherein the host system is coupleable to a server equipped to provide cryptographic data to an engine component within the host system, the engine component including predetermined metadata inaccessible outside the engine.

10. A method of securing electronic content, the method comprising:

interfacing a controller to provide input and output of data; and

coupling a host system to the controller, configuring the host system to present content under predetermined conditions, operating the host system with a navigation protocol, operating a system manager on the host system, the host system operable to:

configure an associations component to be at least partially run by the host system;

configure a translator to provide meanings and generate commands within the host system;

configure at least a first digital rights management (DRM) component to provide encoding and access rules for the content; and

configure a file system component including a file system application programming interface (API) to provide a logical interface between a plurality of components.

11. The method of claim 10 further comprising operating a medium with the host system and the controller, wherein the medium holds the content in files accessible via one or

more of the first DRM component, the file system component, and a second DRM component.

12. The method of claim 10 wherein the content is governed by one of the first DRM component in conjunction with a second DRM component, by the first DRM component, and by the second DRM component in conjunction with the file system component.

13. The method of claim 12 wherein the first DRM component governs access to pre-recorded content on a medium via a secure application programming interface (API).

14. The method of claim 12 wherein the second DRM component governs access to pre-recorded content on a medium via a secure application programming interface (API) associated with the first DRM component.

15. The method of claim 10 wherein the host system is operable with a computer system, the host system preventing access to the content by the computer system.

16. The method of claim 10 wherein the controller is operable with a computer system, the controller preventing access to the content by the computer system.

17. The method of claim 11 wherein the medium operable with the host system and the controller is a media disk.

18. The method of claim 10 wherein the host system further includes an engine component, the engine component including predetermined metadata inaccessible outside the engine, the engine configured to provide a security layer of encryption.

19. The method of claim 10 wherein the host system is coupleable to a server equipped to provide cryptographic data to an engine component within the host system, the engine component including predetermined metadata inaccessible outside the engine.